



Mist Integration with ISE for Guest Access



Table of Contents

<u>FLOW OF GUEST ACCESS VIA RADIUS SERVER USING MAB</u>	3
MIST AP CONFIGURATION	4
WLAN CONFIGURATION	4
AUTHENTICATION POLICY	5
AUTHORIZATION PROFILE	6
URL REDIRECT	7
COA(CHANGE OF AUTHORIZATION)	8
SECOND ACCESS REQUEST AND PERMIT ACCESS	8



Flow of Guest Access via Radius Server using MAB

- 1) Wireless MAB WLAN is created on the Mist AP with MAB being performed via Radius Lookup.
- 2) When a client associated to this WLAN, the the mac address of the client is sent across to the radius server via an ACCESS_REQUEST
- 3) Radius server looks up its database and if the client is not found in the database, sends back a ACCESS_ACCEPT with a redirection URL to the Mist AP
- 4) The client now is provided with limited access to the network which includes access to the BOOTP, DNS and Radius server
- 5) After the client receives an IP, the AP opens a web socket to and listens to any HTTP traffic initiated from the client
- 6) Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
- 7) The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
- 8) Once the client provides necessary info on the URL, the ISE now install this client's mac address in its database and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.
- 9) The Mist AP upon receiving the CoA request – acknowledges the request and sends back the same ACCESS_REQUEST as in step 2.
- 10) At this point - the client is available in the radius server database and hence would be provided with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined.



Mist AP Configuration

WLAN Configuration

- a. Network -> WLAN -> Add WLANs
- b. Enable “MAB by Radius lookup” and “Guest Access with MAB” under it
- c. You can use the Whitelist in order to permit specific subnets/hostnames when the client is in the redirect state (It is optional – if left blank, the radius server is the only IP that is whitelisted for access)

The screenshot shows the Mist AP configuration interface for a WLAN. The left sidebar contains navigation options: CLIENTS, ACCESS POINTS, LOCATION, ANALYTICS, NETWORK, and ORGANIZATION. The main configuration area is divided into several sections:

- SSID:** Abhi-Guest
- Labels:** A plus sign (+) to add labels.
- WLAN Status:** Enabled (selected), Disabled, Hide SSID, No Static IP Devices.
- Radio Band:** 2.4G and 5G, 2.4G, 5G (selected).
- Client Inactivity:** Drop inactive clients after 1800 seconds.
- Geofence:** Contact Mist for Firmware.
- Security:** WPA-2/PSK with passphrase, WPA-2/EAP (802.1X), Open Access (selected), WPA-2/PSK with multiple passphrases, WPA-PSK/TKIP, WPA2-PSK/TKIP, WEP, Multi-mode/PSK with passphrase, Multi-mode/EAP (802.1X), MAC address authentication by RADIUS lookup (selected), Guest Access with Mac Authentication Bypass (selected).
- Web Auth Whitelist:** Allowed Subnets, Allowed Hostnames.

- d. Add the Radius Server of Choice (RadSec is disabled when not used)
 - i. Click on the Radius server and it will provide an option to input the Radius Server details (IP, Port, Shared Secret) which would be the Radius server IP and port details
 - ii. You would also have the option of adding a secondary-server/tertiary servers
 - iii. You will also be edit the order of the preference for servers using the arrow keys place beside them.

The screenshot shows a dialog box titled "RADIUS Authentication Server" with a close button (X) in the top right corner. The dialog contains the following fields:

- Hostname:** 10.2.2.30
- Port:** 1812
- Shared Secret:** xxxxxxxx

At the bottom of the dialog, there are three buttons: "Remove Server" (red), "OK" (blue), and "Cancel" (grey).

a. When a client associates to this WLAN, the access point sends a ACCESS-REQUEST to Radius Server

The packet capture shows an Access-Request (ID=1, L=166) sent from the client (172.24.89.158) to the RADIUS server (155.64.42.55). The packet details include:

- Code: Access-Request (1)
- Packet Identifier: 0x0 (0)
- Length: 166
- Authenticator: b851e5b8fa33809c63ade4179aa727
- Attribute Value Pairs:
 - AVP: l=4 t=User-Name(1): f48c597eb8c6
 - AVP: l=18 t=User-Password(2): Encrypted
 - AVP: l=18 t=User-Password(2): Encrypted
 - AVP: l=6 t=Service-Type(6): Call-Check(10)
 - AVP: l=35 t=Called-Station-Id(30): 5C-5B-35-20-00-03:SYNC-Guest_test
 - AVP: l=6 t=NAS-Port-Type(31): Wireless-002:11(10)
 - AVP: l=19 t=Calling-Station-Id(33): F4-8C-50-7E-00-C6
 - AVP: l=24 t=Connect-Info(177): CONNECT 130mps 002.11b
 - AVP: l=6 t=NAS-IP-Address(4): 172.24.89.158
 - AVP: l=18 t=Message-Authenticator(80): 17d23352f93491677a37bc712299306

b. The packet capture above indicates the ACCESS-REQUEST sent across from the client

The screenshot shows the configuration for the "MAB" authentication policy. The conditions are set to "Wired_MAB OR Wireless_MAB". The actions are configured as follows:

- If Auth fail: REJECT
- If User not found: CONTINUE
- If Process fail: DROP

The policy has 48 hits.

c. The authentication policy on the radius server is tailored to “continue” if the user is not found in the database. This allows the client to get an IP and be placed in the redirect state.

Policy Name	Conditions	Actions	Hits
Wi-Fi_Guest_Access	IdentityGroup-Name EQUALS Endpoint Identity Groups:HotSpot_Endpoints Wireless_MAB	PermitAccess	0
Wi-Fi_Redirect_to_Guest_Login	Wireless_MAB	Guest_Access	47
Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess	0
Default		DenyAccess	0

d. The authorization policy has two policies that will be hit during the process of this guest access flow. The first policy that is hit as indicated above is “Wifi_Redirect_to_Guest_Login” which provides partial access to the client.

- i. Note: Upon successful auth after CoA we hit the second auth indicated as “Wifi_Guest_Access” which provides full access to the client

Authorization Profile

Once we hit the first policy MAB policy on the Radius server, the server responds with an Access-Accept to the Mist AP but also provides a redirect URL which is presented to the client. The policy is created as below in the radius server

The screenshot shows the configuration for an Authorization Profile. On the left is a sidebar with navigation options: Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main area is titled 'Common Tasks' and includes a dropdown for 'Centralized Web Auth' set to 'ACL', with 'ACL_WEBAUTH_REDIRECT' selected. The 'Value' is 'Sponsored Guest Portal (default)'. There are three checkboxes: 'Display Certificates Renewal Message' (checked), 'Static IP/Host name/FQDN' (checked) with the value '10.2.15.254', and 'Suppress Profiler CoA for endpoints in Logical Profile' (unchecked). Below this is the 'Advanced Attributes Settings' section with a 'Select an item' dropdown and a '+' button. The 'Attributes Details' section shows the following configuration:

```

Access Type = ACCESS_ACCEPT
Airspace-ACL-Name = ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=acl=ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://10.2.15.254:port/portal/gateway?sessionId=SessionId&portal=079c670-7159-11e7-a355-005056aba474&daysToExpire=value&action=cwa
    
```

The Radius server response would contain the above URL as shown in the packet capture below.

Note: Although there is an ACL that is presented as well as a part of the response, at Mist, we wouldn't need to configure any ACL/WxLAN policies as we have a built in wall garden policy which provide BOOTP, DNS and ISE server access only to the client.

Time	Source IP	Destination IP	Source Port	Destination Port	Protocol	Length	Info
310	2018-08-17 17:43:22.978274	192.168.8.42	192.168.8.11	204	RADIUS	204	Access-Request(1) (id=12, l=162)
311	2018-08-17 17:43:23.015352	192.168.8.11	192.168.8.42	581	RADIUS	581	Access-Accept(2) (id=12, l=539)
473	2018-08-17 17:43:27.902296	192.168.8.42	192.168.8.11	204	RADIUS	204	Access-Request(1) (id=13, l=162)
474	2018-08-17 17:43:27.949698	192.168.8.11	192.168.8.42	572	RADIUS	572	Access-Accept(2) (id=13, l=530)
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271	CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86	CoA-ACK(44) (id=53, l=44)

```

▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_0e:02:b7 (5c:5b:35:0e:02:b7)
▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.42
▶ User Datagram Protocol, Src Port: 1812, Dst Port: 48218
▼ RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xc (12)
  Length: 539
  Authenticator: b65d47cb334340e451b8815bac804ac0
  [This is a response to a request in frame 310]
  [Time from request: 0.037078000 seconds]
  ▼ Attribute Value Pairs
    ▼ AVP: l=19 t=User-Name(1): 68-EC-C5-09-2E-69
      Type: 1
      Length: 19
      User-Name: 68-EC-C5-09-2E-69
    ▶ AVP: l=67 t=State(24): 52656175746853657373696f6e3a63306138303830623631547452515f53356c5f...
    ▶ AVP: l=78 t=Class(25): 434143533a63306138303830623631547452515f53356c5f...
    ▶ AVP: l=18 t=Message-Authenticator(80): fe260cbc9ae1cdc036963d2cabb09b4
    ▼ AVP: l=45 t=Vendor-Specific(26) v=ciscoSystems(9)
      Type: 26
      Length: 45
      Vendor ID: ciscoSystems (9)
    ▶ VSA: l=39 t=Cisco-AVPair(1): url-redirect=acl=ACL_WEBAUTH_REDIRECT
    ▼ AVP: l=217 t=Vendor-Specific(26) v=ciscoSystems(9)
      Type: 26
      Length: 217
      Vendor ID: ciscoSystems (9)
    ▶ VSA: l=211 t=Cisco-AVPair(1): url-redirect=https://192.168.8.11:8443/portal/gateway?sessionId=c0a8080b61TRQ_SS1_Tna7L54PeAZBQ4kmT6GDGXXPCXRUDm86portal=f0ae43f0-7159-11e7-a355-005056aba474&daysToExpire=value&action=cwa
    
```



URL redirect

- At this stage, client is able to procure an IP.
- The client should initiate an HTTP transaction – by logging into the browser and trying to reach an external URL
- Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
- The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
- Once the client provides necessary info on the URL, **the radius server now installs this client’s mac address in its database** and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.

No.	Time	Source	Destination	Length	Protocol	Size	I X Hate	HSSI	Channel	Info
474	2018-08-17 17:43:27.949698	192.168.8.11	192.168.8.42	572	RADIUS	572				Access-Accept(2) (id=13, l=530)
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86				CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	284	RADIUS	284				Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286				Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=54, l=229)

```

▶ Frame 951: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits)
▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_0e:02:b7 (5c:5b:35:0e:02:b7)
▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.42
▶ User Datagram Protocol, Src Port: 41351, Dst Port: 3799
▼ RADIUS Protocol
  Code: CoA-Request (43)
  Packet identifier: 0x35 (53)
  Length: 229
  Authenticator: 190cde5bd49afdf47bcb87c7245d90
  [The response to this request is in frame 952]
  ▼ Attribute Value Pairs
    ▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.8.42
    ▶ AVP: l=19 t=Calling-Station-Id(31): 68-EC-C5-09-2E-69
    ▶ AVP: l=6 t=Event-Timestamp(55): Aug 17, 2018 17:43:40.000000000 PDT
    ▶ AVP: l=18 t=Message-Authenticator(80): 58413c17b15355502a0551858f0160f4
    ▼ AVP: l=43 t=Vendor-Specific(26) v=ciscoSystems(9)
      Type: 26
      Length: 43
      Vendor ID: ciscoSystems (9)
      ▶ VSA: l=37 t=Cisco-AVPair(1): subscriber:reauthenticate-type=last
    ▼ AVP: l=41 t=Vendor-Specific(26) v=ciscoSystems(9)
      Type: 26
      Length: 41
      Vendor ID: ciscoSystems (9)
      ▶ VSA: l=35 t=Cisco-AVPair(1): subscriber:command=reauthenticate
    ▼ AVP: l=76 t=Vendor-Specific(26) v=ciscoSystems(9)
      Type: 26
      Length: 76
      Vendor ID: ciscoSystems (9)
      ▶ VSA: l=70 t=Cisco-AVPair(1): audit-session-id=c0a8080b61TRQ_S5L_Tna7LS4PeAZBQ4kmT6DGDXXPChRXUDm8
  
```

Note:

- 1) The key observation in the CoA request is that Cisco AV pair Subscriber:Command has the value “reauthenticate”. This is the reason why we are able to authorize a client for the second time around without having to disconnect the client.
- 2) The Cisco AV pair Subscriber:Reauthenticate-type has the value “last” which indicates that the Mist AP should use the same access request as it presented the last time for the client in question.



CoA(Change of Authorization)

We acknowledge this CoA request using a CoA Ack

No.	Time	Source	Destination	Length	Protocol	Size	TX Rate	RSSI	Channel	Info
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86				CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204	RADIUS	204				Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286				Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=54, l=229)

▶ Frame 952: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
 ▶ Ethernet II, Src: Mist_0e:02:b7 (5c:5b:35:0e:02:b7), Dst: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c)
 ▶ Internet Protocol Version 4, Src: 192.168.8.42, Dst: 192.168.8.11
 ▶ User Datagram Protocol, Src Port: 3799, Dst Port: 41351
 ▼ RADIUS Protocol
 Code: CoA-ACK (44)
 Packet identifier: 0x35 (53)
 Length: 44
 Authenticator: de7370fd09f7d5ddceb232f33b2e51f
 [This is a response to a request in frame 951]
 [Time from request: 0.002731000 seconds]
 ▼ Attribute Value Pairs
 ▶ AVP: l=6 t=Event-Timestamp(55): Aug 17, 2018 17:43:40.000000000 PDT
 ▶ AVP: l=18 t=Message-Authenticator(80): 9013d7fde7f0d353e6c1b5de6040b0e9

Second Access Request and Permit Access

- Based on the CoA request – we send the same ACCESS REQUEST back to the client

No.	Time	Source	Destination	Length	Protocol	Size	TX Rate	RSSI	Channel	Info
474	2018-08-17 17:43:27.949698	192.168.8.11	192.168.8.42	572	RADIUS	572				Access-Accept(2) (id=13, l=530)
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86				CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204	RADIUS	204				Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286				Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=54, l=229)

▶ Frame 953: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
 ▶ Ethernet II, Src: Mist_0e:02:b7 (5c:5b:35:0e:02:b7), Dst: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c)
 ▶ Internet Protocol Version 4, Src: 192.168.8.42, Dst: 192.168.8.11
 ▶ User Datagram Protocol, Src Port: 3799, Dst Port: 1812
 ▼ RADIUS Protocol
 Code: Access-Request (1)
 Packet identifier: 0xd (13)
 Length: 162
 Authenticator: 1d058ee7d99027c84015a6ebaed04cf1
 [The response to this request is in frame 956]
 ▼ Attribute Value Pairs
 ▼ AVP: l=14 t=User-Name(1): 68ecc5092e69
 Type: 1
 Length: 14
 User-Name: 68ecc5092e69
 ▼ AVP: l=18 t=User-Password(2): Encrypted
 Type: 2
 Length: 18
 User-Password (encrypted): f4a417644d217877e37f2b11279f45d6
 ▶ AVP: l=6 t=Service-Type(6): Call-Check(10)
 ▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.8.42
 ▶ AVP: l=31 t=Called-Station-Id(30): 5C-5B-35-00-1E-13:jon_ise_new
 ▶ AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
 ▶ AVP: l=19 t=Calling-Station-Id(31): 68-EC-C5-09-2E-69
 ▶ AVP: l=24 t=Connect-Info(77): CONNECT 11Mbps 802.11b
 ▶ AVP: l=18 t=Message-Authenticator(80): 19ef516c6a1089b9e290f69b0f0ceffc

- At this point - the client is available in the radius server database and hence we hit the second policy from the authorization policy perspective.

Policy Name	Condition	Action	Count
Wi-Fi_Guest_Access	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:HotSpot_Endpoints Wireless_MAB	PermitAccess	0
Wi-Fi_Redirect_to_Guest_Login	Wireless_MAB	Guest_Access	47
Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess	0
Default		DenyAccess	0

In the above example – we would meet the criteria for the policy named “Wifi_Guest_Access” since the hotspot clients are stored in the Hotspot_Endpoints Identity Group. Hence the client would be provided



with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined which in this case is "PermitAccess"